REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed January 25, 2005. In the Office Action, claims 1-21 were rejected. Reconsideration in light of the amendments and remarks made herein is respectfully requested. A Request for Continued Examination is being filed with the preliminary amendment.

Applicant respectfully points out that the Advisory Action states that the recitation of the "combination key being used to decrypt a second BIOS area" is not recited in the rejected claims. This is incorrect because claim 1 explicitly claims the following:

> combining the first keying material with a second keying material internally stored within the platform in order *to produce a combination key*; and
> *using the combination key to decrypt* a second BIOS area to recover a second segment of BIOS code. *Emphasis added.*

Applicant has added these limitations into independent claims 12, 15 and 19 and respectfully requests the Examiner to reconsider the allowability of the claimed invention.

Rejection Under 35 U.S.C. § 103

Claims 1-11 were rejected under 35 U.S.C. §103(a) as being unpatentable over England (U.S. Patent No. 6,330,670) in view of Adams (U.S. Patent No. 6,363,485) and Reardon (U.S. Patent No. 6,212,635). Claims 12-21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over England in view of Adams. Applicant respectfully traverses these rejections in their entirety because a *prima facie* case of obviousness has not been established.

A. Claims 1-11

Claims 1-11 were rejected under 35 U.S.C. §103(a) as being unpatentable over England in view of Adams and Reardon. Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988).* Herein, at a minimum, the combined teachings of the cited references do not describe or suggest all the claim limitations set forth in independent claims 1.

Herein, neither England nor Adams nor Reardon, alone or in combination, suggest every limitation set forth in the above-identified claims. For instance, the Office Action states that column 7, lines 45-62 of England teaches an operation to "decrypt a second BIOS area to recover a second segment of BIOS code." Applicant respectfully disagrees with these findings because

such teachings (col. 7, lines 45-62) of England merely describe the general functionality of a CPU (140) having a pair of public and private keys (164). This position is evidenced by the description set forth in column 7, lines 45-62 of England, written as follows:

> The CPU 140 has a processor 160 and also can have a cryptographic accelerator 162. The CPU 140 is capable of performing cryptographic functions, such as signing, encrypting, decrypting, and authenticating, with or without the accelerator 162 assisting in intensive mathematical computations commonly involved in cryptographic functions.
>
> The CPU manufacturer equips the CPU 140 with a pair of public and private keys 164 that is unique to the CPU. For discussion purpose, the CPU's public key is referred to as "K_{CPU} " and the corresponding private key is referred to as "K_{CPU}^{-1} ". Other physical implementations may include storing the key on an external device to which the main CPU has privileged access (where the stored secrets are inaccessible to arbitrary application or operating systems code). The private key is never revealed and is used only for the specific purpose of signing stylized statements, such as when responding to challenges from a content provider, as is discussed below.

There is no teaching or suggestion anywhere in England or in the other cited references for decrypting a second BIOS area, considered to be boot code 717 of FIG. 7B of England, to recover a second segment of BIOS as claimed. This limitation is further refined by dependent claim 3.

The mere fact that Reardon teaches the "recovery of encrypted files" and England teaches the "recovery after encryption" does not suggest the decryption of a second BIOS area as claimed. Withdrawal of the rejection as applied to claim 1 is respectfully requested.

With respect to dependent claims 2-11, Applicant respectfully traverses these rejections as well. Most notably, with respect to claim 3, England (column 11, lines 30-63) does not disclose the loading a BIOS code including a first BIOS area and a second BIOS area. According to claim 3, the first BIOS area is an encrypted first segment of BIOS code and the second BIOS area is an encrypted second segment of BIOS code. Instead, if the Examiner considers the first BIOS area to be equivalent to Basic Boot Code (715) of England and the second BIOS area to be equivalent to Boot Code (717), both of which are not encrypted segments of BIOS code as claimed.

In light of the foregoing, Applicant respectfully requests that the Examiner withdraw the rejection of claims 1-11 under 35 U.S.C. §103(a).

B. Claims 12-21

Claims 12-21 were rejected under 35 U.S.C. §103(a) as being unpatentable over England in view of Adams. Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

For instance, Applicant respectfully submits that neither England nor Adams, alone or in combination, fails to teach or even suggest producing a combination key by combining a first incoming keying material with a second keying material internally stored within the integrated circuit device (or trusted platform module or the platform itself) and *to decrypt a second BIOS area to recover a second segment of BIOS code.* Emphasis added. Instead, as noted above, England merely describe the general public-private key functionality where the second BIOS area, considered by the Examiner as Boot Code 717, does not teach or suggest storage of encrypted data. In addition, Adams teaches production of a secret key (210) based on partial encryption key seed data (218) and sampled biometric input data (224), which has no applicability to recovery of data from BIOS.

Hence, there is no motivation or suggestion for the combination key being used to decrypt a second BIOS area as set forth in independent claims 12, 15 and 19, which is further defined in subsequent dependent claims as a segment of BIOS placed in an encrypted format. In fact, Adams teaches away from the invention because it involves *outputting* the secret key (210) *to* a personal computer (212) or other suitable device that needs the secret key to decrypt encrypted data. Emphasis added. The combination offers not suggestion of decrypting a specific segment of the BIOS code as claimed.

Hence, Applicant respectfully requests the Examiner to reconsider and withdraw the outstanding §103(a) rejection of Claims 12-21.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 4/25/05 By _____

William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☒ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: 4/25/2005

FACSIMILE

☐ *transmitted by facsimile to the Patent and Trademark Office.*

4/25/2005

Susan McFarlane *Date*